OUCH! | 2016 년 07 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- CEO 사기란?
- 보호대책

CEO 사기

CEO 사기란?

사이버범죄자들은 얍삽합니다. 이들은 자신들이 원하는 것을 얻기 위해 지속적으로 새로운 방법을 고안합니다. 가장 효과적인 방법 중 하나가 일반인을 대상으로 공격하는 것입니다. 사이버공격자들은 모든 조직에서 부주의한 사람들이 가장 약한 고리인 것을 알고 있으며, 반면 주의력이 있는 사람들이 조직의 가장 좋은 방어책이 될 수 있다는 사실에 대해서는 잊고 있습니다.

객원 편집자

안젤라 파파스는 톰슨 로이터에서 정보보호 교육 및 인식제고 담당이사이다. 그녀는 피싱에 대해 앰베서더 프로그램, 이러닝 및 직원 교육 업무를 담당하고 있다.

사이버범죄자들은 CEO 사기 또는 사업 이메일해킹(BEC)이라고 불리는 새로운 공격을 개발하였습니다. 이 공격에는 사이버범죄자들이 CEO또는, 회사의 고위임원인 것처럼 사칭합니다. 범죄자들은 직원들에게 이메일을 보내서, 하지 말아야 할 것으로 실행하도록 속입니다. 사이버범죄자들이 회사에 대해서 연구를 하기 때문에, 이러한 유형의 공격은 굉장히 효과적입니다. 범죄자들은 회사의 웹사이트를 검색하여 회사의 위치, 임원진 또는 협력사와 같은 정보를 찾습니다. 그 다음 범죄자들은 SNS, 블로그 등에서 동료직원에 대한 모든 정보를 얻습니다. 일단 범죄자들이 회사의 조직을 알았다면, 그 다음 누구를 대상으로 할 지 특정 직원을 찾습니다. 이 때는 범죄자들은 구체적인 목적에 기반하여 공격 대상을 선정합니다. 만약에 범죄자들이 돈을 얻고자 한다면, 회계 부서 직원을 대상으로 할 것입니다. 만약에 세금 정보를 찾는다면, 인사부서를 대상으로 합니다. 만약에 데이터베이스 서버에 접근하고 싶다면, IT 부서의 누군가를 대상으로 합니다.

일단 범죄자들이 원하는 목표와 대상을 정하면, 공격시나리오를 짭니다. 이 때 주로 스피어 피싱을 이용합니다. 피싱은 공격자들이 수백만 명의 사람들에 이메일을 보내, 사람들은 속여서 어떤 것을 하도록 하는 것입니다. 예를 들어 감염된 첨부문서 및 악성 웹사이트를 클릭하도록 합니다. 스피어 피싱은 피싱과 유사하지만, 수백만 명의 일반적인 사람들에게 보내는 대신 적은 수의 사람을 선택하여 맞춤형 이메일을 보내는 것입니다. 이러한 스피어 피싱 이메일은 굉장히 현실적으로 보이며, 탐지가 쉽지 않습니다. 이러한 이메일은 직장 동료와 상사 등 우리가 알고 있거나 같이 일하는 사람이 보낸 것처럼

CEO 사기

보입니다. 이메일은 동료들이 자주 사용하는 말투/은어도 사용하여 진짜와 같이 보입니다. 범죄자들은 조직의 로고도 사용하고, 공식 서명도 사용합니다. 이러한 이메일에는 보통 굉장히 급한 일이라고 하며, 즉시 행동하도록 하고, 다른 사람들에게 말하지 말라고 요청합니다. 사이버범죄자의 목적은 이렇게 해서 실수를 유도하는 것입니다. 다음은 일반적인 세 가지 공격 시나리오가 입니다.

CEO 사기는 대부분의 보안방어책을 우회할 수 있는 강력한 공격입니다. 극단적으로 우리가 최고의 방어책입니다.

- **송금**: 범죄자들이 돈이 필요합니다. 즉 범죄자들은 회계부서에서 일하는 사람들이 누구인지 또는 회사 자금을 담당하는 팀이 누구인지 파악합니다. 범죄자들은 그 다음 상사로 위장하여 이메일을 보냅니다. 이메일에는 급한 일이 생겨서 어떤 계좌로 즉시 이체해야 한다는 내용이 있습니다.

- **세금 사기**: 범죄자들은 직장동료에 대한 정보를 훔쳐 세금 사기를 위해 직원으로 위장합니다. 범죄자들은 회사를 연구하여 인사부 등 직원정보를 다루는 사람이 누구인 지를 파악합니다. 그 다음 범죄자들은 회사 임원 또는 세무사라고 위장하여 즉시 어떤 문서를 보내달라고 요청합니다.

- **변호사 사칭**: 모든 CEO 사기가 이메일로 이루어 지는 것은 아닙니다. 전화와 같은 다른 방법도 사용될 수 있습니다. 이 시나리오에서는 범죄자들은 회사의 팀장이라고 사칭하여 이메일을 보냅니다. 이 메일에는 변호사가 급한 일로 전화할 것이라고 적혀 있습니다. 그 다음 범죄자들은 변호사인척하며 전화합니다. 범죄자들은 엄청 급한 일이라고 하며. 시간이 굉장히 중요하고 비밀이라고 합니다. 급한 일이라고 하여 사람을 속여서 즉시 행동하도록 하는 것입니다.

보호대책

그렇다면 우리자신과 조직을 보호할 수 있는 방법은 무엇일까요? 가장 좋은 보호대책은 상식적으로 생각하는 것입니다. 만약에 우리가 직장 상사나 동료로부터 메시지를 받는다면, 공정한 것처럼 보이지 않으면 공격일 수 있습니다. 공격을

CEO 사기

알아차릴 수 있는 단서는 굉장히 급하다고 하며, 공정하지 않은 것 저럼 보이거나, 목소리 억양이 좀 다를 수 있다는 것입니다. 다른 단서는 공격자들은 우리가 전에 보지 못한 전화번호나 이메일을 사용하는 것입니다. 또는 유사하지만 완전히 동일하지 않는 것을 사용할 수 있습니다. 의심이 되면 이메일로 답변을 하지 말고, 그 사람에게 직접 전화를 하거나 만나서 이메일을 보내는 지 확인해 보시기 바랍니다. 그리고 절대로 회사의 보안 정책이나 절차를 위반하면 안됩니다. 회사는 자금을 이체하거나 비밀정보를 보낼 때 내부적으로 승인에 관한 정책 또는 절차가 있습니다. 이러한 정책을 위반해도 괜찮다는 요청이 있다면 의심을 해야 합니다. 그리고 실제로 행동으로 옮기기 전에 확인절차를 거쳐야 합니다. 만약에 이러한 요청을 받고 어떻게 할지 모르겠다면, 상사, 회사의 헬프 데스크 또는 보안 팀으로 즉시 연락해 보시기 바랍니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

사회공학:	https://securingthehuman.sans.org/ouch/2014#november2014
피싱:	https://securingthehuman.sans.org//ouch/2015#december2015
악성코드란 무엇인가:	https://securingthehuman.sans.org/ouch/2016#march2016
2단계 인증:	https://securingthehuman.sans.org/ouch/2015#september2015
일일 보안팁:	https://www.sans.org/tip-of-the-day

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역: 진수희(ITL Inc.)